УДК 003.26.09:004.032.24-004.272.3
Вітрук І.В.
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ ПОТОКОВИХ АЛГОРИТМІВ ШИФРУВАННЯ

Науковий керівник: к.т.н., доцент, Луцків А.М.

Алгоритми Grain, Trivium, Bivium-B, HiTag2 та Crypto1, криптостійкість яких досліджуватиметься у даній науковій доповіді, є представниками потокових алгоритмів шифрування.

Потоковим шифром називають симетричний шифр, в якому кожен символ відкритого тексту перетворюється в символ шифрованого тексту в залежності не тільки від використовуваного ключа, але і від його розташування в потоці відкритого тексту. Потоковий шифр реалізує інший підхід до симетричного шифрування, ніж блокові шифри.

Актуальність використання потокових шифрів зумовлена низкою переваг у порівнянні з іншими видами алгоритмів шифрування, а саме: простотою апаратної реалізації, високою швидкістю шифрування (важливо при шифруванні великих потоків інформації), відсутністю ефекту розмноження помилок, який присутній в блокових шифрах.

Потокові шифри мають широке застосування, наприклад:

- у системах захисту інформації комп'ютерних мереж [1];
- у системах стільникового та супутникового зв'язку;
- автомобільних охоронних системах;
- системах аутентифікації осіб на основі RfID-карт тощо.

Алгоритми HiTag2, Grain, Crypto1 застосовуються у системах автомобільної та охоронної сигналізації, смарт-картах та деяких протоколах безпровідних мереж.

Оскільки, використання потокових алгоритмів шифрування є таким популярним, практичним та актуальним, то важливою задачею є перевірка їх надійності — криптоаналіз.

Криптоаналіз – це наука, що займається вивченням криптостійкості алгоритмів шифрування. Криптоаналіз потокових шифрів можна здійснювати багатьма методами: силові атаки, статистичні атаки, аналітичні атаки тощо.

Одним з найбільш ефективних для потокових шифрів є метод алгебраїчного криптоаналізу [2,3]. При алгебраїчному криптоаналізі завдання полягає в знаходжені початкового стану інформаційного повідомлення, заданого деякими ключовими потоками бітів. Метою атаки є відновлення вихідного стану (k0,..., kn−1) з деякими m послідовними бітами гами b0 ... bm−1, шляхом розв'язання багатовимірних рівнянь (швидкі алгебраїчні атаки вимагають послідовних бітів).

В даній науковій доповіді буде досліджено криптостійкість актуальних та важливих в практичній реалізації алгоритмів потокового шифрування, зокрема, методом алгебраїчного криптоаналізу.

1. Криптоанализ алгоритма поточного шифрования RC4 :зб. текстов 8 всерос. научно-практ. конф. / МИФИ. – С., 2001. – 83 с.
2. Mate Soos – CryptoMiniSat2 [Електронний ресурс] - Режим доступу: URL: http://www.msoos.org/cryptominisat2 - Назва з екрану.
3. Grain - A Stream Cipher for Constrained Environments / Martin Hell [and oth.] // International Journal of Wireless and Mobile Computing – 2007 – №1 – С. 86-93.